DISTINGUISHING DIVISION ALGEBRAS BY FINITE SPLITTING FIELDS

DANIEL KRASHEN AND KELLY MCKINNIE

Abstract. This paper is concerned with the problem of determining the number of division algebras which share the same collection of finite splitting fields. As a corollary we are able to determine when two central division algebras may be distinguished by their finite splitting fields over certain fields.

1. Introduction

A major theme in the study of finite dimensional division algebras is determining those field extensions of the center which split the algebra — i.e. such that the algebra becomes isomorphic to a matrix algebra when the scalars are extended to this field extension. Despite the fact that this is one of the major tools used to determine structural information about such algebras, there are still a large number of open questions. In this paper, we examine how much information is given by the finite splitting fields of a central division algebra. To answer this, we determine in certain cases how many distinct division algebras can share the same collection of finite splitting fields, for example, showing that any pair of quaternion algebras over the field $\mathbb{Q}(t)$ which share the same splitting fields must in fact be isomorphic. This particular fact answers a question originally posed to us by Peter Clark, and was our original motivation this line of inquiry. Our paper further generalizes this to show, for example, that given a division algebra D over $\mathbb{Q}(t)$ of prime period p, the collection of division algebras of period p sharing the same splitting field is always finite.

Independent parallel work of Garibaldi-Saltman [GS] and Rapinchuk-Rapinchuk [RR] has also given the above result on quaternion algebras over the field $\mathbb{Q}(t)$. Besides the fact that the methods we use are quite distinct from these other two approaches, the results in these papers differ from ours in two basic ways: First, [GS] is concerned only with quaternion algebras (and symbols in higher cohomology groups), and [RR] is concerned only with period 2 division algebras. Second, they are interested in only maximal subfields, as opposed to finite splitting fields. By focusing on all finite splitting fields, as opposed to simply the maximal subfields, we are able to prove results for more general fields than those arising in [RR], as well as make statements concerning splitting fields for algebras of periods other than 2.

In the course of this paper, we also introduce some new techniques for working with unramified Brauer classes on curves with rational points, for example, showing that such classes always arise as pullbacks of Brauer classes on the Jacobian of the curve via the Abel-Jacobi map (Proposition 3.4).

2. Statement of main results

Definition 2.1
Let k be a field and let $\alpha, \beta \in \mathrm{Br}(k)$. We write $\alpha \equiv \beta$ if for every finite field extension ℓ/k we have α_ℓ is split if and only if β_ℓ is split. This defines an equivalence relation on the elements of $\mathrm{Br}(k)$ and we let $\|\alpha\|$ denote the equivalence class of α.

If $\|\alpha\| \neq \|\beta\|$ for some α, $\beta \in \mathrm{Br}(k)$, then there exists a finite field extension ℓ/k such that ℓ splits one of α or β, but not the other. Therefore, if $\|\alpha\| \neq \|\beta\|$ we say that α and β can be distinguished via splitting fields. Our main result is to say that if one knows a bound for the order of the sets $\|\alpha\|$ over a field k, one may also understand the potential size of these sets over $k(t)$.

Theorem 2.2
Let k be a field and p a prime integer not equal to the characteristic of k. Let $\alpha \in \mathrm{Br}(k(t))[p]$ and suppose that the class α is ramified at r distinct closed points. Then

(1) *if all $\alpha_0 \in \mathrm{Br}(k)[p]$ satisfy $\#\|\alpha_0\| \leq N$ for some integer N, then*
$$\|\alpha\| \leq N(p-1)^r.$$
(2) *if all $\alpha_0 \in \mathrm{Br}(k)[p]$ satisfy $\#\|\alpha_0\| < \infty$, then $\#\|\alpha\| < \infty$.*

Remark 2.3
If k is a higher local field, for example, an iterated Laurent series field $k_0((t_1))\cdots((t_m))$ where k_0 is finite, local, or algebraically closed, then one may show that the p-torsion part of the Brauer group, $\mathrm{Br}(k)[p]$, is finite for any p, and in particular, the hypotheses of Theorem 2.2(1) will automatically hold for $N = |\mathrm{Br}(k)[p]|$. A description of when $\mathrm{Br}(k)[2]$ is finite is given in [Efr97] in the case the characteristic of k is not 2. We note also that the weaker conditions of Theorem 2.2(2) hold in the case that k is a global field.

Corollary 2.4
Let k be a field of characteristic not 2, such that for all $\alpha_0 \in \mathrm{Br}(k)[2]$, we have $\#\|\alpha_0\| = 1$. Then for all $\alpha \in \mathrm{Br}(k(t))[2]$, $\#\|\alpha\| = 1$.

In particular, this show that all the 2-torsion elements in $\mathrm{Br}(\mathbb{Q}(t))$ may be distinguished via their finite splitting fields, a question originally posed to us by Peter Clark. This theorem is a consequence of the proceeding results, for which we use the following notation:

For a closed point x in a curve X, $\kappa(x)$ denotes the residue field, and for a Brauer class $\alpha \in k(X)$ unramified at x, we let $\alpha|_x$ denote the specialization of α to the closed point x. One may intepret this concretely by choosing A to be a Azumaya algebra over the local ring $\mathcal{O}_{X,x}$ such that $A \otimes_{\mathcal{O}_{X,x}} k(X)$ represents the class α, and then defining $\alpha|_x$ to be the class of $A \otimes_{\mathcal{O}_{X,x}} \kappa(x)$.

The proof of Theorem 2.2 will depend on the following two theorems.

Theorem 2.5
Let k be a field and p a prime integer not equal to the characteristic of k. Suppose that $\alpha, \beta \in \mathrm{Br}(k(t))$ such that $\alpha \equiv \beta$. Then for every closed point $x \in \mathbb{P}^1(k)$, if we write $\mathrm{ram}_x(\alpha) = (L/\kappa(x), \sigma)$ and $\mathrm{ram}_x(\beta) = (M/\kappa(x), \tau)$ then $L \cong M$ as extensions of $\kappa(x)$.

Theorem 2.6 (*Distinguish classes with distinguishable specializations*)
Suppose $\alpha, \beta \in \mathrm{Br}(k(t))$ with $\alpha \neq \beta$, and suppose there is a rational point $x \in (\mathbb{P}^1_k)^{(1)}$ such that $\mathrm{ram}_x \alpha = \mathrm{ram}_x \beta = 0$ and $\beta|_x \not\equiv \alpha|_x$. Then $\beta \not\equiv \alpha$.

The main content of the remainder of the sections of the paper will be to prove Theorem 2.5 (on page 10) and Theorem 2.6 (on page 8). Before doing so, we first illustrate how these theorems may be used to prove Theorem 2.2.

Proof of Theorem 2.2. Let $\alpha, \beta \in \mathrm{Br}(k(t))[p]$. For any closed point $x \in \mathbb{P}^1_k$, let $\mathrm{ram}_x(\alpha) = (L_x/\kappa(x), \sigma)$. By Theorem 2.5, if $\beta \in \|\alpha\|$, then for every closed point $x \in X$, if $\mathrm{ram}_x(\beta) = (M/\kappa(x), \tau)$ then $M \cong L_x$ as extensions of $\kappa(x)$. Therefore, $\tau = \sigma^i$ for some $1 \leq i \leq p-1$ and α and β ramifiy at the same set of closed points. Let $\{x_j\}$ be the set of closed points at which α ramifies. For each of the $(p-1)^r$ possible sequences $(i_1, \ldots, i_r)$ with $1 \leq i_j \leq p-1$, let

$$\|\alpha\|_{(i_1,\ldots,i_r)} = \{\beta \in \|\alpha\| \mid \mathrm{ram}_{x_j} \beta = (L_x/k(x), \sigma^{i_j}) \text{ for all } 1 \leq j \leq r\}$$

Then, $\|\alpha\| = \bigcup \|\alpha\|_{(i_1,\ldots,i_r)}$ with the union taken over all possible $(p-1)^r$ sequences. To prove part (1), it is only left to show that $\#\|\alpha\|_{(i_1,\ldots,i_r)} \leq N$ and for this we use Theorem 2.6.

In the case that k is infinite, we may choose $x \in \mathbb{P}^1(k)$ such that $\mathrm{ram}_x \alpha = \mathrm{ram}_x \beta = 0$. We show that $\#\|\alpha\|_{(i_1,\ldots,i_r)} \leq \#\|\alpha|_x\|$. Note first that $|_x : \|\alpha\|_{(i_1,\ldots,i_r)} \to \mathrm{Br}(k)$ is injective. This follows since any two elements $\beta_1, \beta_2 \in \|\alpha\|_{(i_1,\ldots,i_r)}$ have the exact same ramification sequence and therefore, by the Auslander-Brummer-Faddeev sequence, $\beta_1 = \beta_2 + \gamma$ for a constant class $\gamma \in \mathrm{Br}(k)$. If $\beta_1|_x = \beta_2|_x$ then $\gamma|_x = \gamma$ is trivial, implying that $\beta_1 = \beta_2$. In the case that k is finite, it follows immediately from the Auslander-Brummer-Faddeev sequence (see e.g., [GS06, 6.9.3]) that $\#\|\alpha\|_{(i_1,\ldots,i_r)} = 1$.

Assume by way of contradiction that $\#\|\alpha\|_{(i_1,\ldots,i_r)} > \#\|\alpha|_x\|$. Then, since the specialization map $|_x$ is injective, $\beta|_x \notin \|\alpha|_x\|$ for some $\beta \in \|\alpha\|_{(i_1,\ldots,i_r)}$. By Theorem 2.6 we can distinguish between α and β using finite dimensional splitting fields, that is, $\beta \notin \|\alpha\|_{(i_1,\ldots,i_r)}$, a contradiction. Therefore, $\#\|\alpha\|_{(i_1,\ldots,i_r)} \leq N$ and $\#\|\alpha\| \leq (p-1)^r N$.

To prove part (2) we use the terminology from above and set

$$M = \max\{\#\|\alpha\|_{(i_1,\ldots,i_r)}\}.$$

where the maximum is taken over all possible $(p-1)^r$ sequences. As stated above, for any rational point $x \notin \{x_j\}$, $\#\|\alpha\|_{(i_1,\ldots,i_r)} \leq \#\|\alpha|_x\| < \infty$, so M is a finite number. Then $\#\|\alpha\| = \sum \|\alpha\|_{(i_1,\ldots,i_r)} \leq (p-1)^r M < \infty$. □

3. Distinguishing Brauer classes via branched covers

Lemma 3.1
Let $\phi : Y \to X$ be a branched cover such that there exists a k-rational point $y \in Y(k)$ and let $x = \phi(y)$. Then,

1. *For any non-trivial constant class $\beta \in \mathrm{Br}(k) \subseteq \mathrm{Br}(k(X))$, $\beta_{k(Y)} \neq 0$.*
2. *If $\phi : Y \to X$ is unramified at y then for any class $\alpha \in \mathrm{Br}(k(X))$, $\mathrm{ram}_y \alpha_{k(Y)} = \mathrm{ram}_x \alpha$.*

Proof. For part (1), consider the commutative diagram

$$\begin{array}{ccccccc} \mathrm{Br}(k) & \hookrightarrow & \mathrm{Br}(X) & \hookrightarrow & \mathrm{Br}(k(X)) & \xrightarrow{\mathrm{ram}_x} & H^1(k,\mathbb{Q}/\mathbb{Z}) \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \phi^*} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle e\cdot\mathrm{res}} \\ \mathrm{Br}(k) & \hookrightarrow & \mathrm{Br}(Y) & \hookrightarrow & \mathrm{Br}(k(Y)) & \xrightarrow{\mathrm{ram}_y} & H^1(k,\mathbb{Q}/\mathbb{Z}), \end{array} \tag{3.1}$$

where e is the ramification index of ϕ at y. The arrows $\mathrm{Br}(k) \hookrightarrow \mathrm{Br}(X)$ and $\mathrm{Br}(k) \hookrightarrow \mathrm{Br}(Y)$ are injections because of the existence of sections given by the rational points. Therefore, $k(Y)$ cannot split β. Part (2) follows from the right hand side of the commutative diagram (3.1),(see [Sal99]) and the fact that $e = 1$ since $\phi : Y \to X$ is unramified at y. □

Although our goal is to prove statements about Brauer classes over $k(t)$, the function field of $\mathbb{P}^1_k$, other curves and their Jacobians will naturally arise in the process. We will therefore shift focus for a while and consider the ramification and splitting behavior of Brauer classes of curves over more general curves.

Let X be a smooth projective curve over k containing a rational point $x \in X(k)$. Let $\phi : X \to \mathrm{Jac}\, X$ be the Albanese map taking x to $[0]$, the identity element. Throughout this section we will set $J = \mathrm{Jac}\, X$. The next two lemmas collect facts about X and J which we use in Lemma 3.5 to produce a cover of X which makes Brauer classes on X constant.

3.1. **Make unramified.**

Lemma 3.2 (*Make it unramified*)
Let k be a field and X a smooth projective k curve. Let $\alpha \in \mathrm{Br}(k(X))[m]$ with $(m, char(k)) = 1$ and let D be the ramification locus of α. Assume there exists $x \in X(k)$, with $\mathrm{ram}_x(\alpha) = 0$. Then, there exists a branched cover $\psi : Y \to X$ and a rational point $y \in Y(k)$ such that

(1) *$\psi(y) = x$, and*
(2) *$\alpha_{k(Y)}$ is unramified at all $y \in Y^{(1)}$ so that $\alpha_{k(Y)} \in \mathrm{Br}(Y)[m]$.*

Proof. Choose a closed point $b \neq x$ in X, with b not in the support of D. We wish to find a rational function on X which is regular away from the point b, which vanishes on the ramification locus D with only simple zeroes, and which is nonzero at the rational point x. Such a function would exactly correspond to a global section of $\mathscr{L}(Nb - D)$ which is also not a section of $\mathscr{L}(Nb - D - x)$ or $\mathscr{L}(Nb - D - d)$ for any d in the support of D.

Choose $N > (2g - 2 + 2\deg(D))$ where g is the genus of X, which in particular ensures that

$$\deg(Nb - D), \deg(Nb - D - x), \deg(Nb - D - d) > 2g - 2,$$

Therefore, $l(K - Nb - D - a) = l(K - Nb) = 0$ where K is the the class of the canonical divisor (see [Har77, IV.1.3.3]). By Riemann-Roch,

$$\begin{aligned} l(Nb - D - z) &= \deg(Nb - D - z) + 1 - g \\ &< \deg(Nb - D) + 1 - g \\ &= l(Nb - D). \end{aligned}$$

For $z = x$ or z a closed point in the support of D. In particular, by choosing N sufficiently large we find that

$$\emptyset \neq \Gamma\left(\mathscr{L}(Nb - D)\right) \setminus \left(\Gamma\left(\mathscr{L}(Nb - D - x)\right) \cup \bigcup_{d \in supp(D)} \Gamma\left(\mathscr{L}(Nb - D - d)\right) \right)$$

That is, there is a global section f of $\mathscr{L}(Nb - D)$ with the germ $f_x \notin \mathfrak{m}_{X,x}$ and with only simple zeros on D.

Let $f(x)$ be the image of f_x in $\mathcal{O}_{X,x}/\mathfrak{m}_{X,x} \cong k$. Set

$$L = k(X)[T]/(T^m - ff(x)^{m-1}).$$

Since every closed point $d \in \operatorname{supp}(D)$ has multiplicity 1, our choice of f ensures $f \in \mathfrak{m}_{X,d} - \mathfrak{m}_{X,d}^2$ and further, since $f(x) \in k \subset \mathcal{O}_{X,d}$ is a unit, $ff(x)^{m-1} \in \mathfrak{m}_{X,d} - \mathfrak{m}_{X,d}^2$. Therefore, by Eisenstein's criterion, the polynomial $T^m - ff(x)^{m-1} \in \mathcal{O}_{X,d}[T]$ is irreducible. In particular, L is a field and T is integral over $\mathcal{O}_{X,d}$ for all $d \in \operatorname{supp}(D)$.

Let Y be the normalization of X in L with morphism $\psi : Y \to X$. We show that Y satisfies the condition of the lemma. Let $p \in X$ be a closed point. If $\operatorname{ram}_p \alpha = 0$, then for any point $q \in Y$ lying over p, $\operatorname{ram}_q \alpha_{k(Y)} = 0$. If $\operatorname{ram}_p \alpha \neq 0$ then $p \in \operatorname{supp}(D)$. Let $q \in Y$ with $\psi(q) = p$. Let π_p be a uniformizer for $\mathcal{O}_{X,p}$ so that $ff(x)^{m-1} = \pi_p u$ with u a unit in $\mathcal{O}_{X,p}$. Let v_q be the valuation of $\mathcal{O}_{Y,q}$ extending that of $\mathcal{O}_{X,p}$. Then $v_q(T^m) = mv_q(T) = v_q(\pi_p) = 1$. Since $[L : k(X)] = m$, it follows that the point q has ramification index $e_q = m$. Therefore, by the standard commutative diagram

$$\begin{array}{ccc} \operatorname{Br}(k(X)) & \xrightarrow{\operatorname{ram}_p} & H^1(k(p), \mathbb{Z}/m\mathbb{Z}) \\ \downarrow & & \downarrow e_q \\ \operatorname{Br}(L) & \xrightarrow{\operatorname{ram}_q} & H^1(k(p), \mathbb{Z}/m\mathbb{Z}) \end{array}$$

$\operatorname{ram}_q \alpha_L = m \cdot \operatorname{ram}_p \alpha = 0$.

It is only left to show that there exists a k-rational point in Y lying over $x \in X(k)$. To do this we compute the fiber Y_x of Y over x. First we note that for any $p \notin \operatorname{supp}(D)$, $ff(x)^{m-1} \in \mathcal{O}_{X,p} - \mathfrak{m}_{X,p}$ is a unit. Moreover, by assumption m is a unit in $k \subset \mathcal{O}_{X,p}$. Therefore the morphism $\operatorname{Spec}\left(\mathcal{O}_{X,p}[T]/(T^m - ff(x)^{m-1})\right) \to \operatorname{Spec} \mathcal{O}_{X,p}$ is étale and in particular, $\mathcal{O}_{X,p}[T]/(T^m - ff(x)^{m-1})$ is integrally closed and hence the integral closure of $\mathcal{O}_{X,p}$ in L. In particular,

$$\begin{aligned} Y_x &= \operatorname{Spec}\left((\text{Int. Clos.}_L \mathcal{O}_{X,x}) \otimes_{\mathcal{O}_{X,x}} \frac{\mathcal{O}_{X,x}}{\mathfrak{m}_x} \right) \\ &= \operatorname{Spec}\left(\frac{k[T]}{T^m - f(x)^m} \right) \\ &= \operatorname{Spec} k \times \operatorname{Spec}\left(\frac{k[T]}{g(T)} \right) \end{aligned}$$

where $T^m - f(x)^m = (T - f(x))g(T)$ and $g(f(x)) \neq 0$. This shows that Y_x has a k-rational point and hence that there is a k-rational point lying over x. $\square$

3.2. **Make constant.**

Lemma 3.3
Let V be a smooth projective k-variety containing a rational point $v \in V(k)$. Then we have a short exact sequence

$$0 \to \mathrm{Br}(k) \to \mathrm{Br}(\overline{V}/V) \to H^1(k, \mathrm{Pic}\,\overline{V}) \to 0$$

arising from the E_2-terms of the Hochschild-Serre spectral sequence for V.

Proof. See for example, [Sko01] Corollary 2.3.9. If we write

$$E_{p,q}^2 = H^p(k, H^q(\overline{V}, \mathbb{G}_m) \implies H^{p+q}(V, \mathbb{G}_m) = E_{p+q}$$

then the above sequence may be identified with the terms in the spectral sequence as:

$$0 \to E_{2,0}^2 \to \left[\ker\left(E_2 \to E_{0,2}^2\right)\right] \to E_{1,1}^2 \to 0$$

□

Proposition 3.4 ($\mathrm{Br}(J)$ ***surjects onto*** $\mathrm{Br}(X)$**)**
The pullback map $\phi^* : \mathrm{Br}(\overline{J}/J) \to \mathrm{Br}(X)$ is surjective.

Proof. Using the fact that pullback of cohomology classes induces a morphism of Hochschild-Serre spectral sequences

$$\begin{array}{ccc} H^p(k, H^q(\overline{J}, \mathbb{G}_m)) & \Longrightarrow & H^{p+q}(J, \mathbb{G}_m) \\ \downarrow & & \downarrow \\ H^p(k, H^q(\overline{V}, \mathbb{G}_m)) & \Longrightarrow & H^{p+q}(V, \mathbb{G}_m) \end{array}$$

combined with Lemma 3.3, we see that this morphism of spectral sequences yields a morphism of short exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Br}(k) & \longrightarrow & \mathrm{Br}(\overline{J}/J) & \longrightarrow & H^1(k, \mathrm{Pic}\,\overline{J}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Br}(k) & \longrightarrow & \mathrm{Br}(\overline{X}/X) & \longrightarrow & H^1(k, \mathrm{Pic}\,\overline{X}) & \longrightarrow & 0 \end{array} \tag{3.2}$$

From the short exact sequence

$$0 \to \mathrm{Pic}^0 X \to \mathrm{Pic}\, X \to \mathbb{Z} \to 0,$$

we obtain an isomorphism $H^1(k, \mathrm{Pic}^0\,\overline{X}) \cong H^1(k, \mathrm{Pic}\,\overline{X})$. Since ϕ^* induces an isomorphism $\mathrm{Pic}_0\,\overline{J} \cong \mathrm{Pic}_0\,\overline{X}$, we may use the commutative diagram

$$\begin{array}{ccc} H^1(k, \mathrm{Pic}^0\,\overline{J}) & \xrightarrow[\cong]{\phi^*} & H^1(k, \mathrm{Pic}^0\,\overline{X}) \\ \downarrow & & \downarrow{\scriptstyle \cong} \\ H^1(k, \mathrm{Pic}\,\overline{J}) & \xrightarrow{\phi^*} & H^1(k, \mathrm{Pic}\,\overline{X}) \end{array}$$

to verify that the pullback map induces a surjection $H^1(k, \mathrm{Pic}\,\overline{J}) \to H^1(k, \mathrm{Pic}_0\,\overline{X})$.

By Tsen's Theorem, $\mathrm{Br}(k(\overline{X})) = 0$. Therefore, $\mathrm{Br}(\overline{X}) \subseteq \mathrm{Br}(k(\overline{X}))$ is also trivial ([Mil80], IV2.6), and in particular, we may identify $\mathrm{Br}(\overline{X}/X) = \mathrm{Br}(X)$.

It now follows from a diagram chase using diagram (3.2) that the pullback map $\mathrm{Br}(\overline{J}/J) \to \mathrm{Br}(X)$ is surjective. □

For any integer n, let $\widetilde{X}_n$ be the fiber product

$$\begin{array}{ccc} \widetilde{X}_n & \xrightarrow{q} & J \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle n} \\ X & \xrightarrow[\phi]{} & J \end{array} \tag{3.3}$$

where n is the multiplication by n map and as always, $J = \mathrm{Jac}\, X$ and $\phi : X \to J$ is the Albanese map given by the rational point $x \in X(k)$. Since the multiplication by n map is étale, p is an étale covering.

Lemma 3.5 (*Pulling back to* $\widetilde{X}_n$.)
Let $\widetilde{X}_n$ be given as above.

(1) *Let $\alpha \in \mathrm{Br}(X)[m]$. Then $p^*\alpha \in \mathrm{Br}(\widetilde{X}_{2m})$ is a constant class.*
(2) *Let $x \in X(k)$ be a rational point. Then for any n, there exists a k-rational point $\tilde{x} \in \widetilde{X}_n(k)$ with $p(\tilde{x}) = x$.*

Proof. (1) By the surjectivity of ϕ^* given in Proposition 3.4 there exists $\beta \in \mathrm{Br}(J)$ such that $\phi^*(\beta) = \alpha$. Let $\bar{\beta} \in H^1(k, \mathrm{Pic}\,\overline{J})$ be the image of β. To show that $(2m)^*(\beta) \in \mathrm{Br}(J)$ is constant it is enough to show that $\overline{(2m)^*\beta} = 0$ in $H^1(k, \mathrm{Pic}\,\overline{J})$. This will follow from the commutativity of

$$\begin{array}{ccc} \frac{\mathrm{Br}(\overline{J}/J)}{\mathrm{Br}(k)} & \xrightarrow{\cong} & H^1(k, \mathrm{Pic}\,\overline{J}) \\ {\scriptstyle n^*}\downarrow & & \downarrow{\scriptstyle n^*} \\ \frac{\mathrm{Br}(\overline{J}/J)}{\mathrm{Br}(k)} & \xrightarrow{\cong} & H^1(k, \mathrm{Pic}\ \overline{J}) \end{array}$$

for all $n \in \mathbb{Z}$, which follows from the naturality of the Hochschild-Serre spectral sequence. Here the map n^* on the right hand side is the map on cohomology gotten from $n^* : \mathrm{Pic}\ \overline{J} \to \mathrm{Pic}\ \overline{J}$, the map pulling back line bundles.

By e.g., [Mum70, pg 59, Corollary 3], for a line bundle $\mathcal{L}$ on J, $n^*(\mathcal{L}) = \mathcal{L}^{\frac{n^2+n}{2}} \otimes (-1)^*\mathcal{L}^{\frac{n^2-n}{2}}$. Notice that the map

$$\begin{aligned} (2m)^* : \mathrm{Pic}\ J &\to \mathrm{Pic}\ J, \\ \mathcal{L} &\mapsto \mathcal{L}^{m(2m+1)} \otimes (-1)^*\mathcal{L}^{m(2m-1)} \end{aligned}$$

factors as $(2m)^* = f \circ g$ where $g(\mathcal{L}) = \mathcal{L}^m$ and $f(\mathcal{L}) = \mathcal{L}^{2m+1} \otimes (-1)^*(\mathcal{L}^{2m-1})$. Consequently $(2m)^* : H^1(k, \mathrm{Pic}\ \overline{J}) \to H^1(k, \mathrm{Pic}\,\overline{J})$ also factors as $f \circ g$, where g is multiplication by m. Therefore, since $\bar{\beta}$ has order dividing m (since $\alpha \in \mathrm{Br}(X)[m]$), $(2m)^*(\bar{\beta}) = 0$. In other words, $(2m)^*(\beta)$ is a constant class. Using the notation from diagram (3.3), $p^*\alpha = q^*(2m)^*\beta$, thus we see $p^*\alpha$ is also a constant class.

(2) By the definition of ϕ, $\phi(x) = [0] \in J$ where x is our rational point. Therefore, by the definition of the fiber product, to produce a rational point of $\widetilde{X}_n(k)$, we need only produce a rational point of J which maps to $[0]$ under n. We simply take the origin itself, since $n[0] = [0]$ for all $n \in \mathbb{Z}$. □

For simplicity we state an immediate corollary.

Corollary 3.6 (*Make unramified classes constant*)
Let $\alpha \in \mathrm{Br}(X)[m]$. Then there is an étale cover of curves $p : \widetilde{X} \to X$ and a rational point $\tilde{x} \in \widetilde{X}(k)$ so that $p(\tilde{x}) = x$ and $p^*(\alpha) \in \mathrm{Br}(k)$ is a constant class.

Lemma 3.7 (*Make it constant*)
Let X/k be a smooth projective curve with $x \in X(k)$, and $\alpha \in \mathrm{Br}(k(X))[m]$ with $\gcd(m, \mathrm{char}\, k) = 1$ and $\mathrm{ram}_x(\alpha) = 0$. There exists a branched cover $\phi : Y \to X$ such that

(1) *$\alpha_{k(Y)}$ is constant,*
(2) *there is a $y \in Y(k)$ such that ϕ is unramified at y and $x = \phi(y)$.*

Proof. By Lemma 3.2 there exists a branched cover $\psi : Y \to X$ and a rational point $y \in Y(k)$ so that $\psi(y) = x$ and $\alpha_{k(Y)} \in \mathrm{Br}(Y)[m]$. So, without loss of generality, we may assume $\alpha \in \mathrm{Br}(X)[m]$, where X is a smooth projective curve over k with rational point x. We are then done by Corollary 3.6 □

We may now complete the proof of Theorem 2.6:

Theorem (*2.6*)
Suppose $\alpha, \beta \in \mathrm{Br}(k(t))$ with $\alpha \neq \beta$, and suppose there is a rational point $x \in (\mathbb{P}^1_k)^{(1)}$ such that $\mathrm{ram}_x \alpha = \mathrm{ram}_x \beta = 0$ and $\beta|_x \not\equiv \alpha|_x$. Then $\beta \not\equiv \alpha$.

Proof. Using Lemma 3.7, once for the class α and then again for the pullback of the class β to the resulting cover, we may find a branched cover $\phi : Y \to \mathbb{P}^1_k$ such that both $\alpha_{k(Y)}$ and $\beta_{k(Y)}$ are constant classes and such that there is a k-rational point $y \in Y(k)$ with $\phi(y) = x$. Then $\alpha_{k(Y)}|_y = \alpha|_x$ and $\beta_{k(Y)}|_y = \beta|_x$ and therefore, $\alpha_{k(Y)} = (\alpha|_x)_{k(Y)}$ and $\beta_{k(Y)} = (\beta|_x)_{k(Y)}$.

By hypothesis $\beta|_x \not\equiv \alpha|_x$ and therefore, modulo switching α and β, there exists a finite field extension L/k such that $(\alpha|_x)_L = 0 \neq (\beta|_x)_L$. Since Y has a rational point, $\mathrm{Br}(L) \to \mathrm{Br}(L(Y))$ is injective and so it follows that we have $0 = \alpha_{L(Y)} \neq \beta_{L(Y)}$. □

4. Distinguishing ramified classes from constant classes

Lemma 4.1 (*Make ramification occur at a rational point*)
Let $\alpha \in \mathrm{Br}(k(t))[m]$ where m is not divisible by $p = \mathrm{char}\, k$ and assume $\mathrm{ram}_x \alpha = (L/k(x), \sigma)$ for some closed point $x \in X$. Then there is a $k(x)$-rational point x' in $X_{k(x)}$ lying over x and, for any such point x', we have $\mathrm{ram}_{x'} \alpha = (L/k(x), \sigma^{p^n})$ for some n.

Proof. Without loss of generality, we may assume that $\mathrm{ram}_x \alpha \neq 0$. Let $k' = k(x)$ be the residue field of the point x, and let $x' \in \mathbb{P}^1_{k'}$ be a k' rational point lying over x. The lemma

follows from the standard commutative diagram

$$\begin{array}{ccc} \mathrm{Br}(k(t))' & \xrightarrow{\mathrm{ram}_x} & H^1(k', \mathbb{Q}/\mathbb{Z})' \\ \Big\downarrow{\scriptstyle \mathrm{res}} & & \Big\downarrow{\scriptstyle e} \\ \mathrm{Br}(k'(t))' & \xrightarrow{\mathrm{ram}_{x'}} & H^1(k', \mathbb{Q}/\mathbb{Z})' \end{array}$$

and the fact that $e = [k' : k]_i$, is the inseparability degree of k'/k see e.g. [GMS03, 9.19]. □

Lemma 4.2 (*Distinguish between ramified and constant*)
Let p be a prime with $(\mathrm{char}\, k, p) = 1$ and let $\alpha, \beta \in \mathrm{Br}(k(X))[p]$ be classes such that

(1) *α is ramified at a rational point $x \in X(k)$ and,*
(2) *β is a constant class (i.e., $\beta \in \mathrm{Br}(k)[p] \subseteq \mathrm{Br}(k(X))$).*

Then $\alpha \not\equiv \beta.\beta_L$ is split and the other is not.

Proof. Since neither α, β, nor the ramification of α at x will be split by a prime to p extension, we may assume without loss of generality that $\mu_p \subset k^*$. Let ω be a primitive p-th root of unity. Let $t \in k(X)$ be a uniformizer for the local ring $\mathcal{O}_{X,x}$ at x. Assume to begin with that $\alpha = (a, t)$ is a symbol with $a \in k^*$ a representative of the ramification $\mathrm{ram}_x\, \alpha \in H^1(k, \mathbb{Z}/p\mathbb{Z}) \cong k^*/(k^*)^p$. Let Y be a model of the extension $L = k(X)[s]/(s^p + ta^{-1})$ over X (we can take, Y to be the normalization of X in L). Then one may check that since $\mathcal{O}_{X,x}[s]/(s^p + ta^{-1})$ is integrally closed, Y has a k-rational point lying over x (at $s = t = 0$). Futher, we note that $u = t/s$ satisfies $u^p = -at^{p-1}$, and so the extension L splits α since $(a, t)_L = (a, au^p)_L = (a, -at^p)_L = (a, -a)_L = 0$. By Lemma 3.1(1), since Y has a rational point, $L = k(Y)$ does not split β.

We now consider the general case $\alpha \in \mathrm{Br}(k(X))[p]$ with ramification at x. Write $\alpha = \gamma + (a, t)$ where γ is unramified at x and as above $a \in k^*$ satisfies $\bar{a} = \mathrm{ram}_x\, \alpha$. By Lemma 3.7 there exists a branched cover $Y \to X$ with a rational point $y \in Y(k)$ lying over x so that

(1) $\gamma_{k(Y)}$ is constant,
(2) $\mathrm{ram}_q\, \alpha_{k(Y)} = \mathrm{ram}_p\, \alpha = \bar{a}$, and
(3) β is not split by $k(Y)$ because Y has a rational point, but is still (of course) a constant class.

So we may assume without loss of generality that $\alpha = \gamma + (a, t) \in \mathrm{Br}(k(X))[p]$ where γ is a constant class. Note that since the cover $Y \to X$ is unramified at y it follows that t pulls back to a uniformizer at y. By the Merkurjev-Suslin Theorem, we may fix a representation for γ as a sum of symbols, $\gamma = \sum_{i=1}^{n} (a_i, b_i) \in H^2(k, \mu_p)$.

Suppose that for some i, the subgroups of $k^*/(k^*)^p$ generated by a_i and a do not coincide. We claim that the ramification of the symbol (a, t) is not split by the extention $\ell_i = k(\sqrt[p]{a_i})$. Since the cover $X_{\ell_i} \to X$ is unramified, we obtain a commutative diagram

$$\begin{array}{ccc} \mathrm{Br}(k(X)) & \xrightarrow{ram} & H^1(k, \mu_p) \\ \Big\downarrow{\scriptstyle res} & & \Big\downarrow{\scriptstyle res} \\ \mathrm{Br}(\ell_i(X_{\ell_i})) & \xrightarrow[ram]{} & H^1(\ell_i, \mu_p) \end{array}$$

In particular, by Kummer theory, it follows that the extensions ℓ_i and $k(\sqrt[p]{a})$ are linearly disjoint, implying that the ramification of (a, t) remains nontrivial at the ℓ_i-rational point

lying over x. We proceed to extend scalars to each such ℓ_i successively (and replacing k by ℓ_i). This cannot split the ramification of (a,t) and hence will not split the class α. If β becomes split, then we have shown $\alpha \not\equiv \beta$ and so we are done.

After extending scalars as above, we may assume that β is not split and that for each (a_i, b_i) in the decomposition of γ, a_i has the same p-power residue class as a^r for some r. In particular, we find $(a_i, b_i) = (a^r, b) = (a, b^r)$, and so without loss of generality, we may combine all such symbols to write

$$\alpha = (a,t) + (a,b) = (a,bt)$$

for some $b \in k^*$. However in this case we have reduced to the original one considered since bt is another uniformizer for the rational point $x \in X(k)$. That is, $\alpha \not\equiv \beta$ since there exists a finite extension $L/k(X)$ which splits α without splitting β. □

We may now complete the proof of Theorem 2.5

Theorem (*2.5*)
Let k be a field and p a prime integer. Suppose that $\alpha, \beta \in \mathrm{Br}(k(t))$ such that $\alpha \equiv \beta$. Then for every closed point $x \in X$, if we write $\mathrm{ram}_x(\alpha) = (L/\kappa(x), \sigma)$ and $\mathrm{ram}_x(\beta) = (M/\kappa(x), \tau)$ then $L \cong M$ as extensions of $\kappa(x)$.

Proof. By Lemma 4.1, we may replace k by a finite extension, and assume that $x \in \mathbb{P}^1(k)$. Suppose that $M \ncong L$ as extensions of k. Since they are degree p extensions, it follows that they are linearly disjoint and so by extending scalars from k to M we may assume that in fact β is unramified at x and α is ramified at x. By Lemma 3.7, we may find a branched cover $\phi : X \to \mathbb{P}^1_k$ with a rational point x' lying over x, and such that $\beta_{k(X)}$ is a constant class and ϕ is unramified at x'. By Lemma 3.1, it follows that $\alpha_{k(X)}$ is ramified at x'. Finally, we may conclude from Lemma 4.2 that $\alpha \not\equiv \beta$ as desired. □

References

[Efr97] Ido Efrat. On fields with finite Brauer groups. Pacific J. Math., 177(1):33–46, 1997.

[GMS03] Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre. Cohomological invariants in Galois cohomology, volume 28 of University Lecture Series. American Mathematical Society, Providence, RI, 2003.

[GS] S. Garibaldi and D. Saltman. On division algebras having the same maximal subfields. Preprint available at http://arxiv.org/abs/0906.5137v1.

[GS06] Philippe Gille and Tamás Szamuely. Central simple algebras and Galois cohomology, volume 101 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2006.

[Har77] Robin Hartshorne. Algebraic geometry. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Mil80] James S. Milne. Étale cohomology, volume 33 of Princeton Mathematical Series. Princeton University Press, Princeton, N.J., 1980.

[Mum70] David Mumford. Abelian varieties. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[RR] A.S. Rapinchuk and I.A. Rapinchuk. On division algebras having the same maximal subfields. Preprint available at http://arxiv.org/abs/0910.3368v2.

[Sal99] David J. Saltman. Lectures on division algebras, volume 94 of CBMS Regional Conference Series in Mathematics. Published by American Mathematical Society, Providence, RI, 1999.

[Sko01] Alexei Skorobogatov. Torsors and rational points, volume 144 of Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, 2001.